UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/711,323	11/09/2000	Alfonso de Jesus Valdes	10454-014002	6879

52197 7590 08/17/2009

Wall & Tong, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
08/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/711,323	VALDES ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 10-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 10-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 26 May 2009.

2. Claims 1-5 and 10-12 are pending in the application.

3. Claims 1-5 and 10-12 have been rejected.

4. Claims 6-9 and 13 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-5 and 10-12 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5 and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 (hereinafter Purtell) in view of Fox et al U.S. Patent No. 7,096,502 B1 (hereinafter Fox).

As to claim 1, Purtell discloses a method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by of the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, the belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably at intervals of one to thirty seconds, each firewall 100 obtains a substantially current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100 of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting is based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to a suspicious activity in the intrusion detection system is improved (i.e. In a preferred embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The

> CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better policy decisions that allow for enhanced throughput between the internal network 102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

As to claim 2, Purtell discloses that the first sensor and the second sensor are different types of sensors (i.e. firewalls and proxy servers) [column 3, lines 33-50].

As to claim 3, Purtell discloses that the first sensor is a probabilistic sensor (i.e. Referring to FIG. 4, a CCB update packet 400 is shown. In a preferred embodiment, the CCB update packet 400 is the data structure through which a firewall 100 shares its CCBs 300 with the other firewalls 100 on the internal network 102. The CCB update packet 400 includes one or more CCBs 300. The one or more CCBs 300 in the CCB update packet 400 are copies of the one or more CCBs 300 located in the computer which originated the CCB update packet 400. The CCB update packet 400 includes a packet header 402 identifying the CCB update packet 400 and providing other information useful for properly routing the CCB update packet 400 to the appropriate firewall or firewalls 100. The use of a packet header to transmit a data packet is known in the art.) [Figure 4 and accompanying description].

As to claim 4, Purtell discloses a method of reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the second sensor (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably at intervals of one to thirty seconds, each firewall 100 obtains a substantially current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100 of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor, so

that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system (i.e. In a preferred embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better policy decisions that allow for enhanced throughput between the internal network 102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

As to claim 5, Purtell discloses a method of enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably

at intervals of one to thirty seconds, each firewall 100 obtains a substantially current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100 of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system (i.e. In a preferred embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better

policy decisions that allow for enhanced throughput between the internal network 102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

As to claim 10, Purtell discloses a sensor device containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, the belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably at intervals of one to thirty seconds, each firewall 100 obtains a substantially current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100

of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved (i.e. In a preferred embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better policy decisions that allow for enhanced throughput between the internal network 102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

As to claim 11, Purtell discloses a computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a

monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by of the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably at intervals of one to thirty seconds, each firewall 100 obtains a substantially current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100 of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system (i.e. In a preferred

embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better policy decisions that allow for enhanced throughput between the internal network 102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

As to claim 12, Purtell discloses a sensor device containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor (i.e. By sharing CCBs 300 on a relatively frequent basis, preferably at intervals of one to thirty seconds, each firewall 100 obtains a substantially

current picture of the overall state of the internal network 102. If one firewall 100 suddenly requires additional band width to handle data requests through it, its network peers preferably reduce the data traffic rate through themselves to prevent network saturation. Those network peers have the knowledge to reduce that data traffic rate based on the shared connection state data 306 within the CCBs 300 they have received from the firewall 100 requiring additional bandwidth. Because the CCBs 300 provide knowledge to a firewall 100 of the behavior of its network peers, throughput can be improved by allowing each firewall 100 to better adjust the traffic through itself to reduce or prevent network saturation.) [column 11, lines 10-39]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent service or resource appears suspicious to the intrusion detection system (i.e. In a preferred embodiment, each firewall 100 adjusts data traffic passing through it based on the contents of the CCBs 300 stored within it. The CCBs 300 provide an individual firewall 100 with data regarding the overall conditions on the internal network 102. The policy decisions made by the firewall 100 are based on concerns including security, bandwidth, and resource utilization. By utilizing data regarding the state of the internal network 102, the firewall 100 can make better policy decisions that allow for enhanced throughput between the internal network

102 and the external network 110. In a preferred embodiment, each firewall 100 periodically reviews the CCBs 300 stored within it to determine of the overall state of the internal network 102. Preferably, that individual firewall 100 then adjusts the data traffic through it, based on the data traffic through its network peers.) [column 10 line 61 to column 11 line 9].

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431